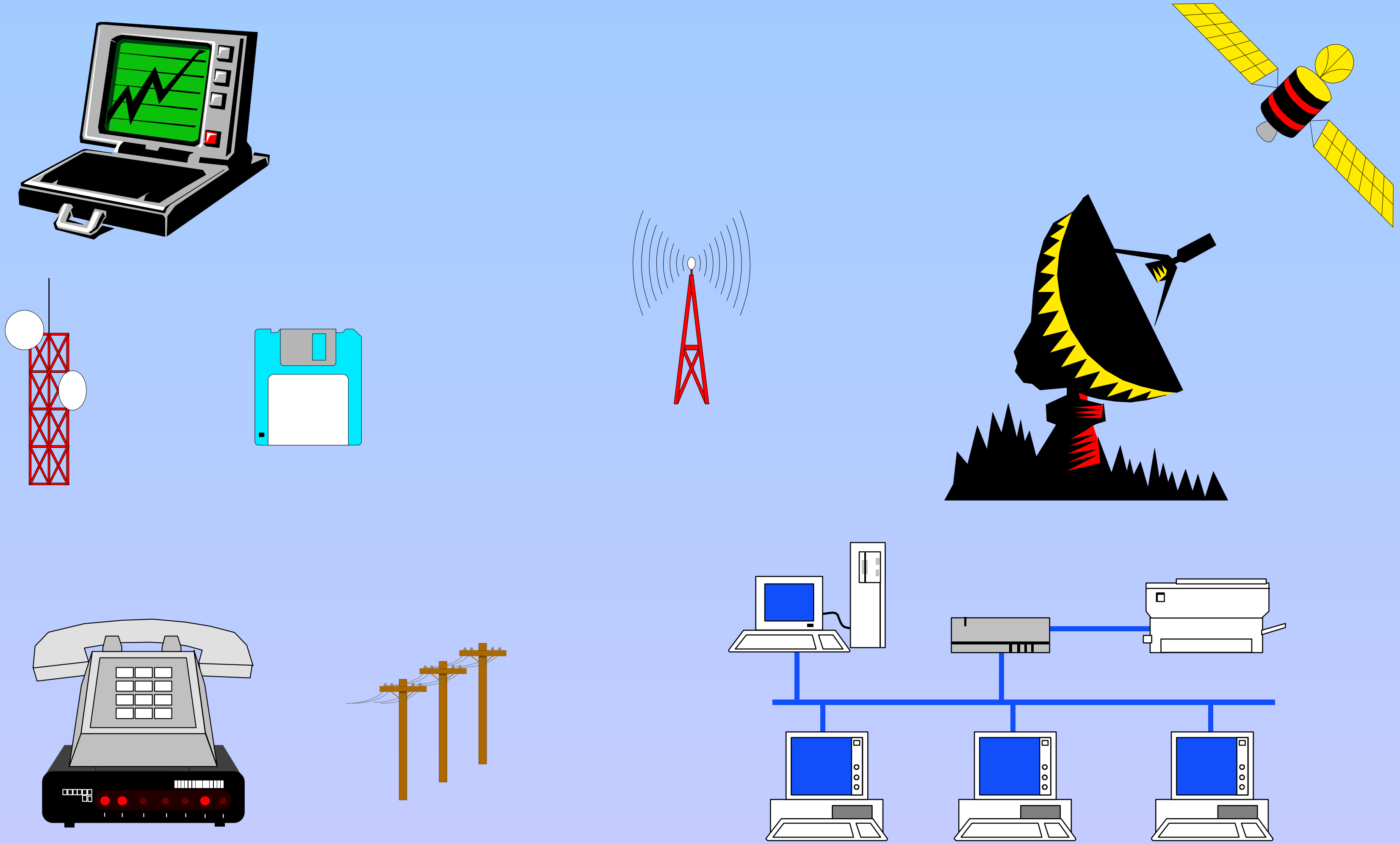
DON INFOSEC PRINCIPLES AND PROCEDURES FOR THE USER

COURSE OBJECTIVES

- Identify Navy INFOSEC Policies
- Risk Management
- Virus Prevention
- Application of Core Values in INFOSEC

WHAT IS INFOSEC?



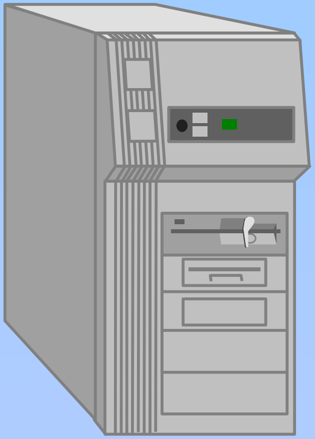
INFOSEC Considerations

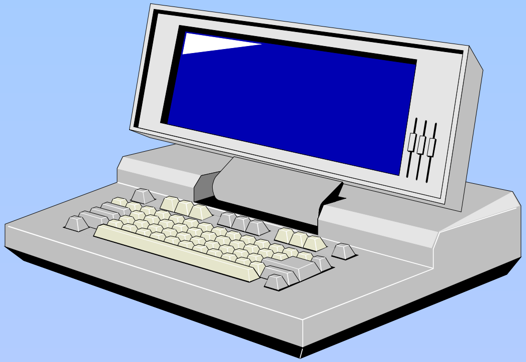
- Hardware and Software
- Information
- Documentation
- Personnel
- Telecommunications

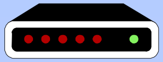
Introduction to Risk Management

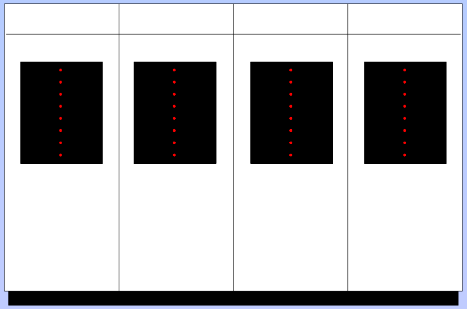
- Terminology
  - Asset
  - Risk
  - Threat
  - Vulnerability
  - Countermeasure

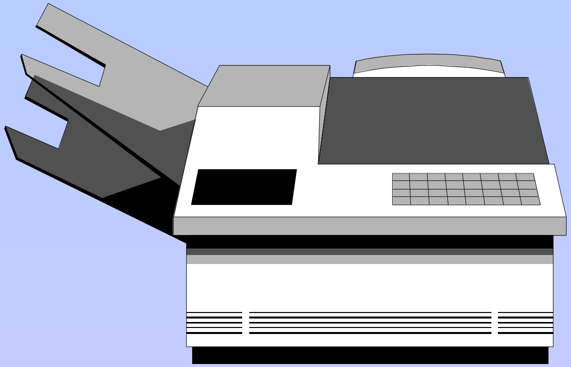
Asset











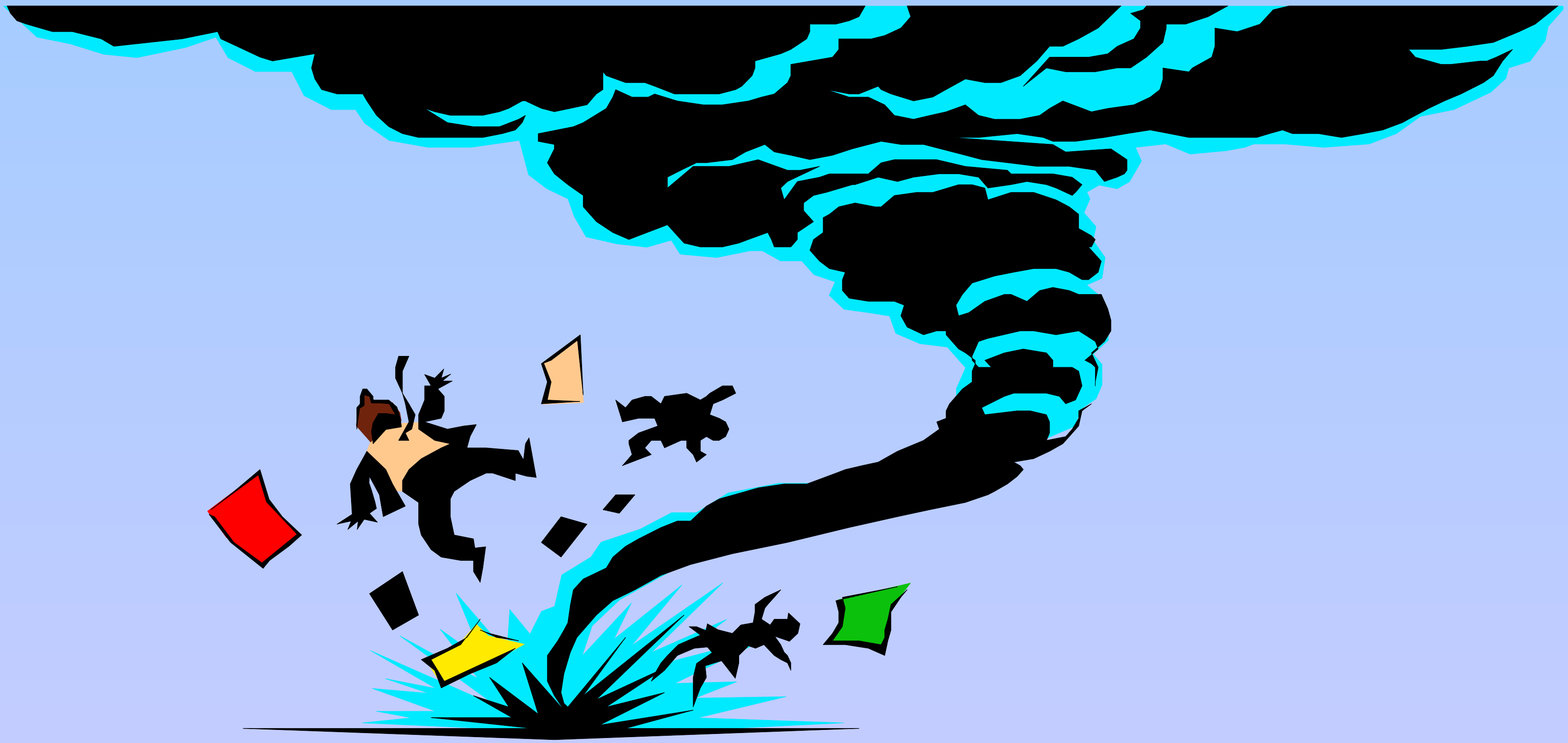
Risk

Threat

Capabilities, Intentions, and Attack Methods of Adversaries to Exploit, or Any Circumstance or Event With the Potential to Cause Harm to Information or an Information System

(NAVO P-5239-02)

Natural Threats



Man-Made Threats

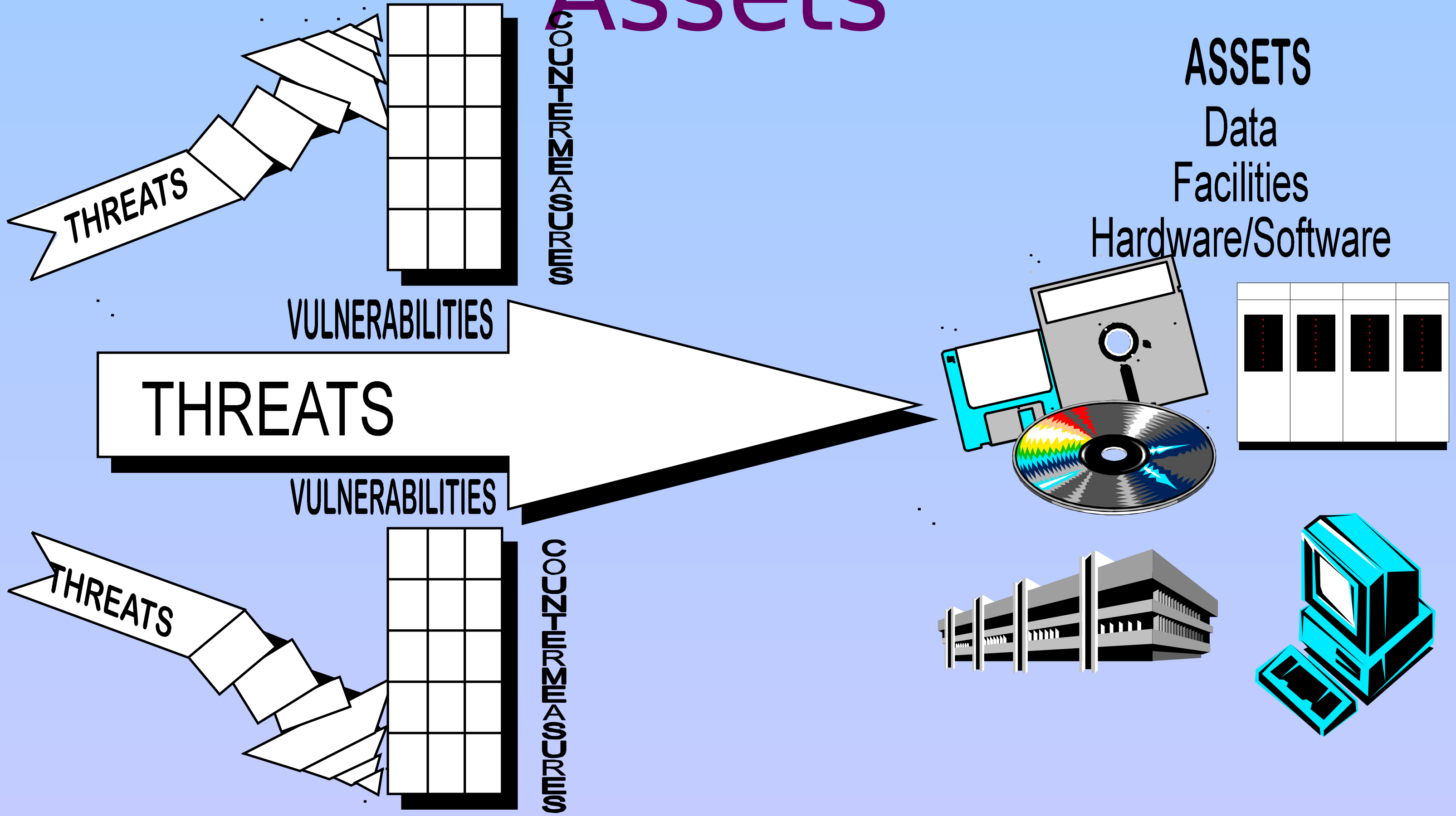
- Internal
- External
- Environmental
- Technical

Vulnerability

- A Weakness in an Information System or Cryptographic System or Components That Could Be Exploited to Violate System Security Policy (NAVSO P-5239-02)

Safeguard/Countermeasure

Threats, Vulnerabilities, Countermeasures and Assets

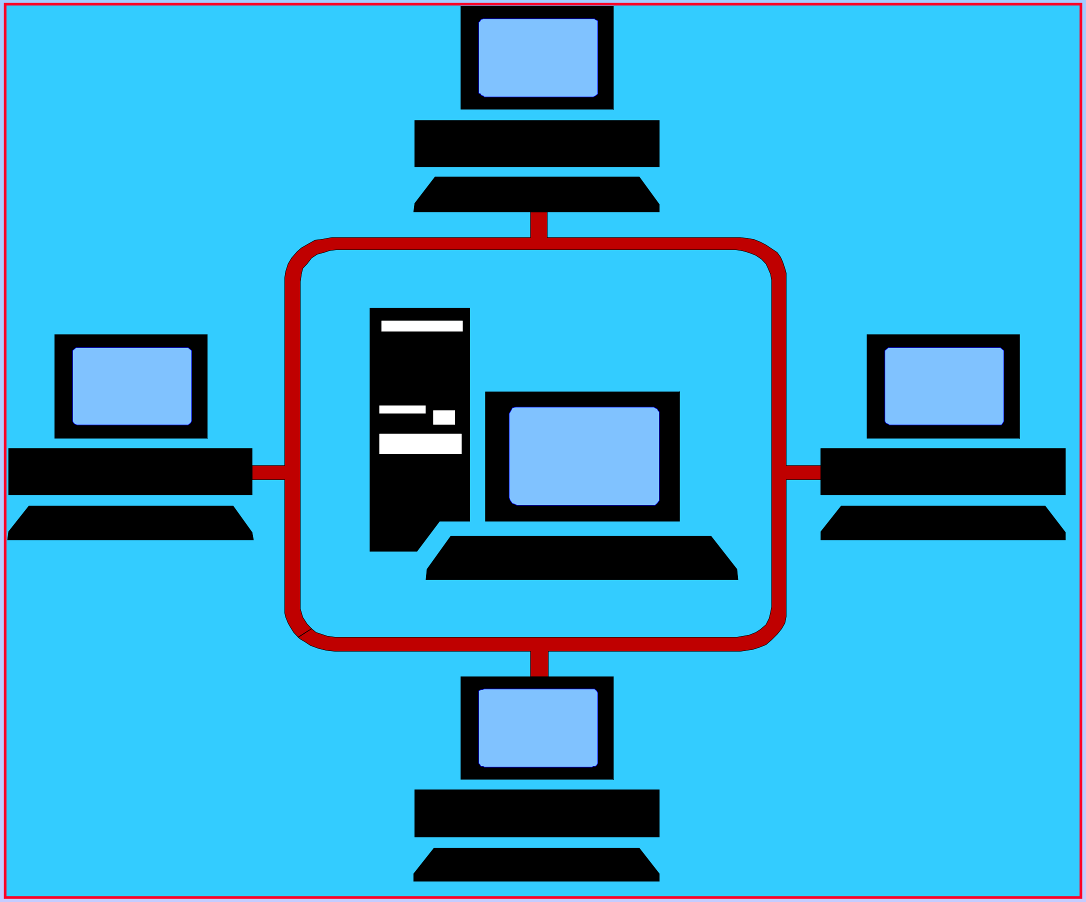


Risk Management

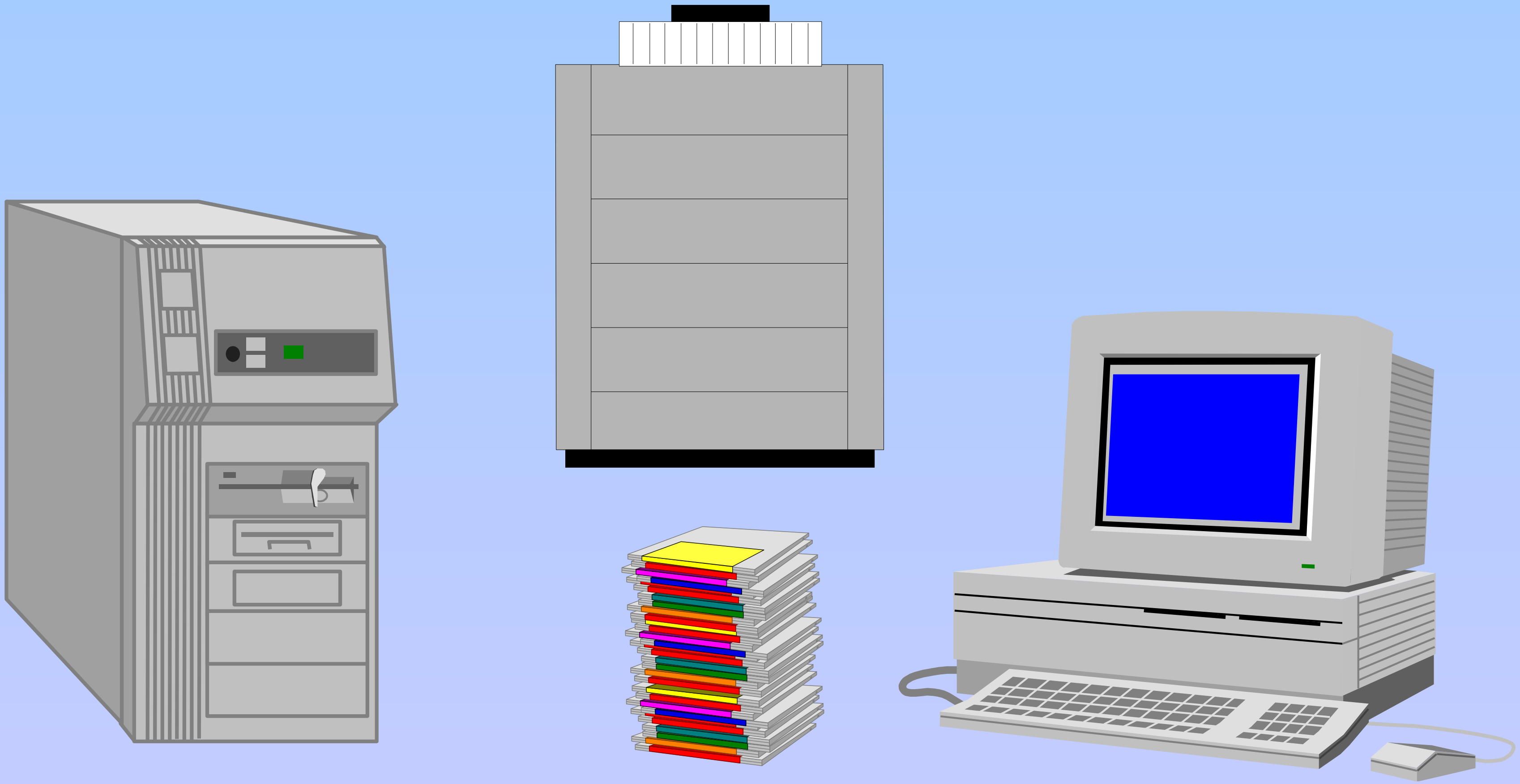
- The Process Concerned With the Identifying, Control, and Minimizing of Security Risks in Information Systems
- Contingency Planning
- Security Test & Evaluation
- Accreditation

Introduction to Network Security

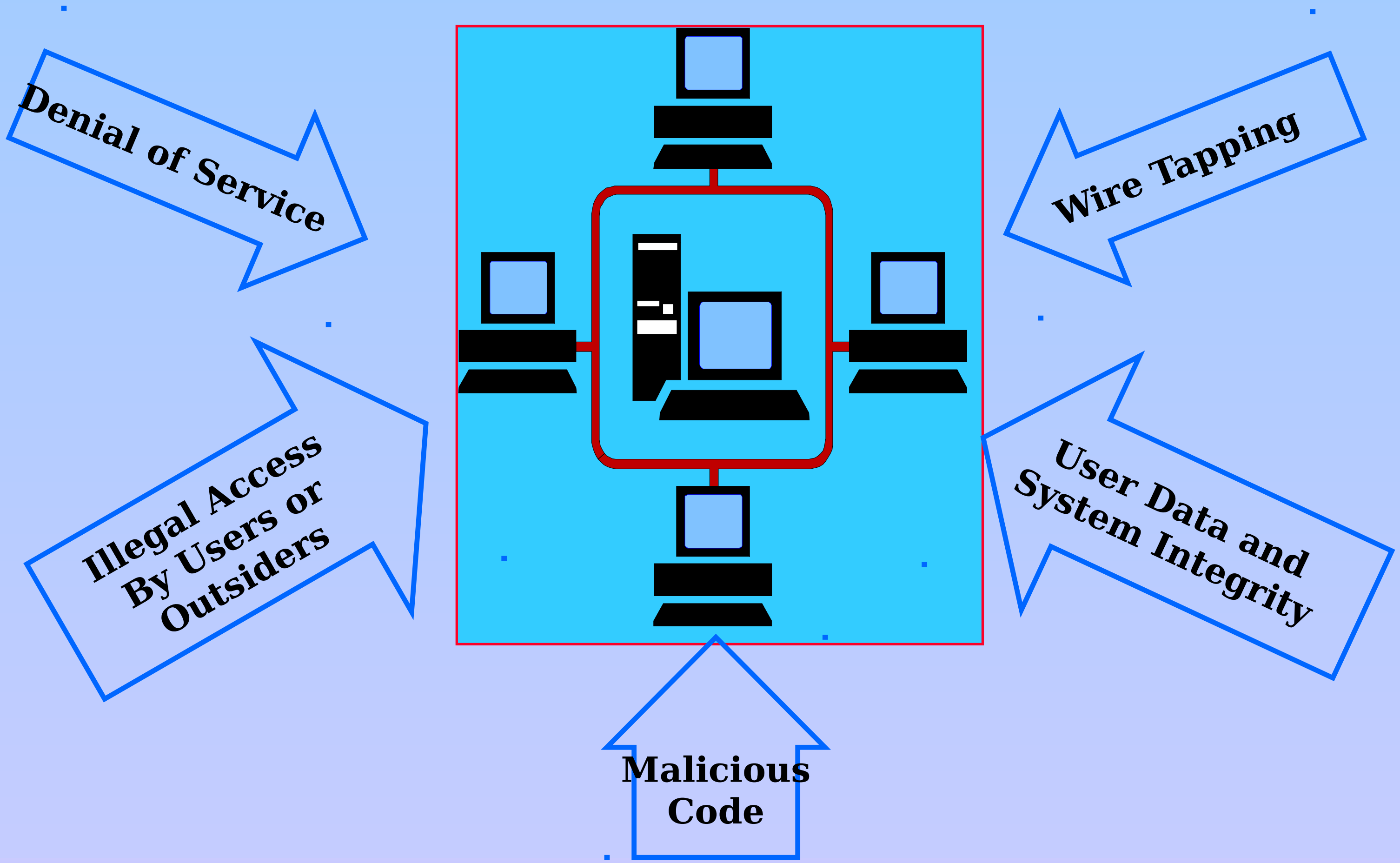
LAN Definition



LAN Components



Network Vulnerabilities and Risks



Denial of Service

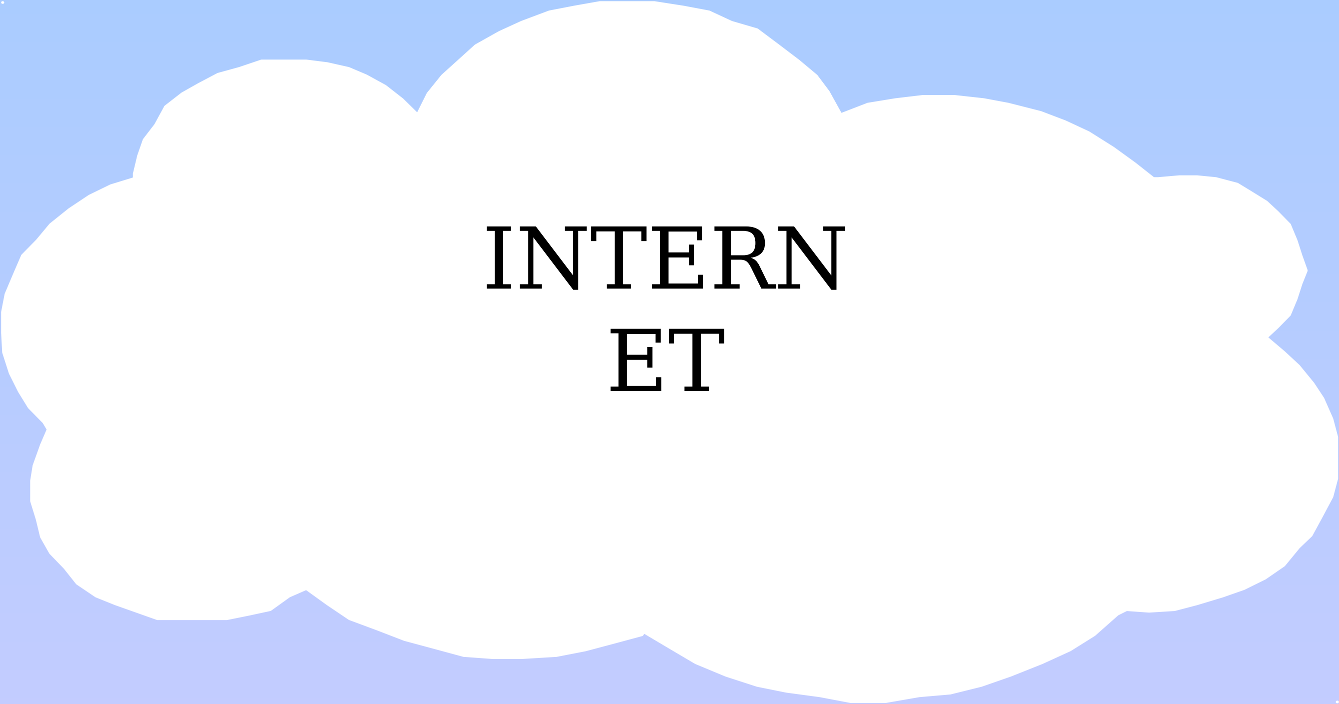
Wire Tapping

Illegal Access By Users or Outsiders

User Data and System Integrity

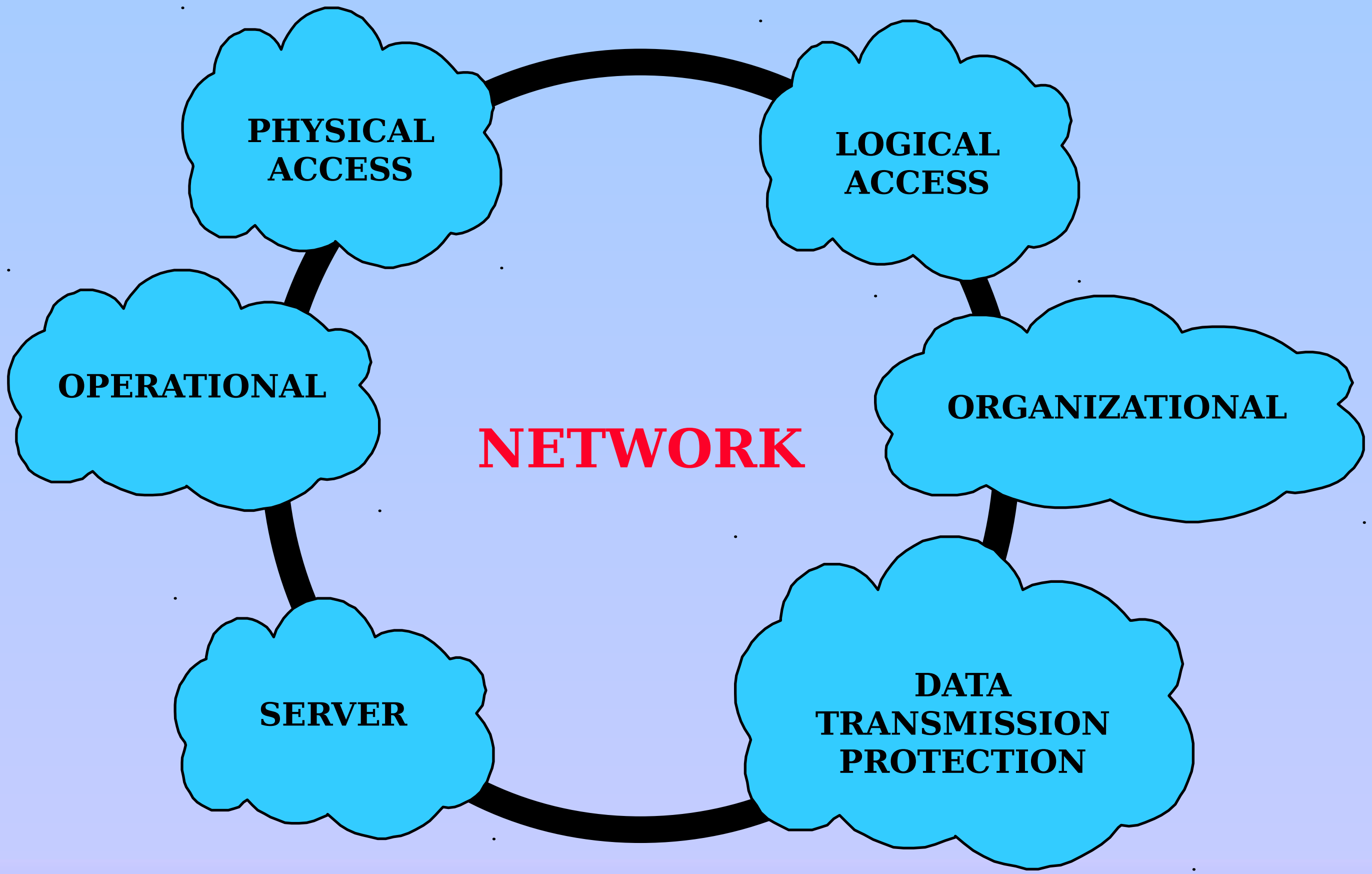
Malicious Code

The Internet



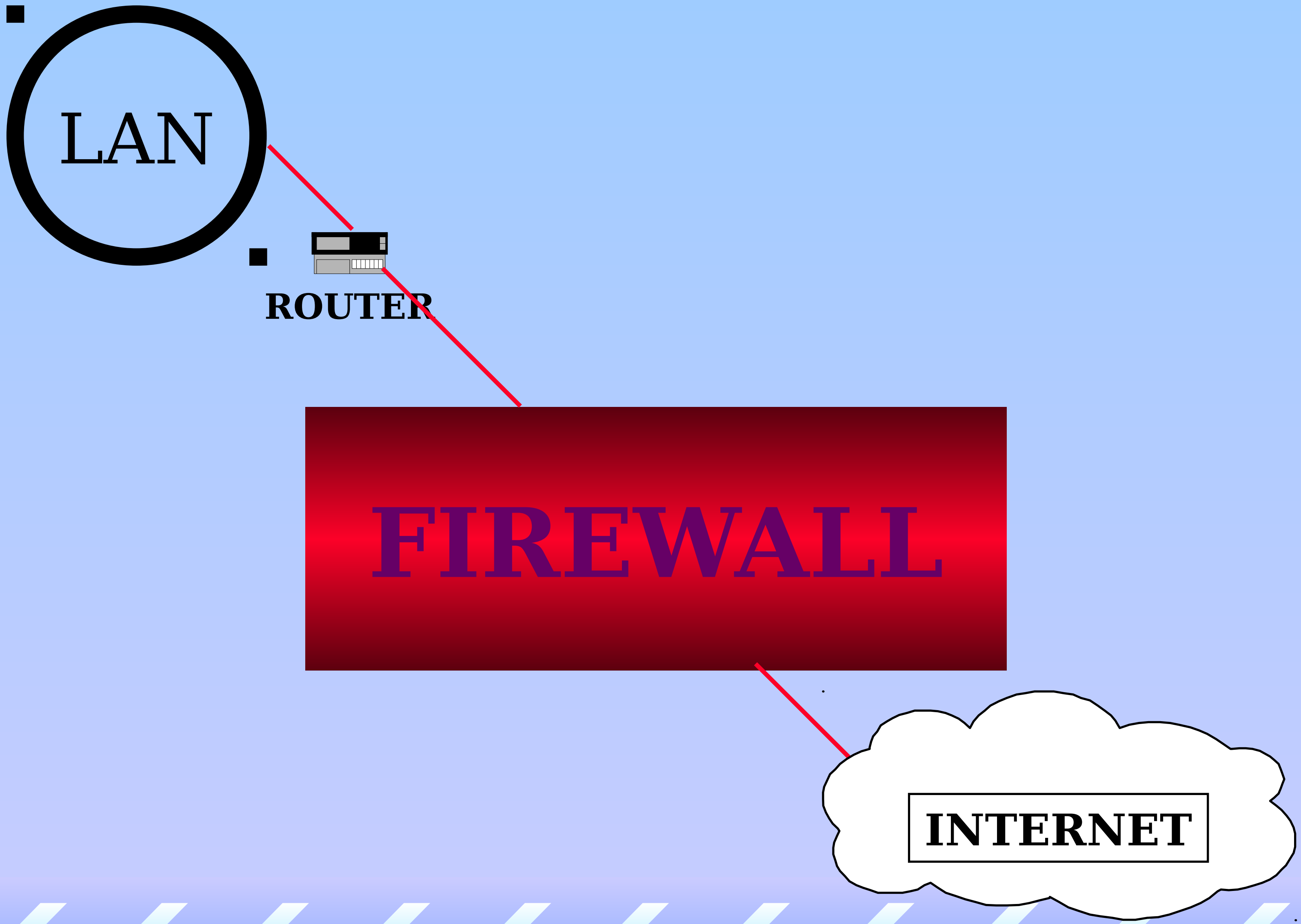
INTERNET

Network Security Controls



Network Security Services

- Centralized Management of Backups
- File Locking and Encryption Capability
- Access Control
- Authentication



LAN

ROUTER

FIREWALL

INTERNET

DOD Warning Banner

USE OF THIS OR ANY OTHER DOD INTEREST COMPUTER SYSTEM CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES

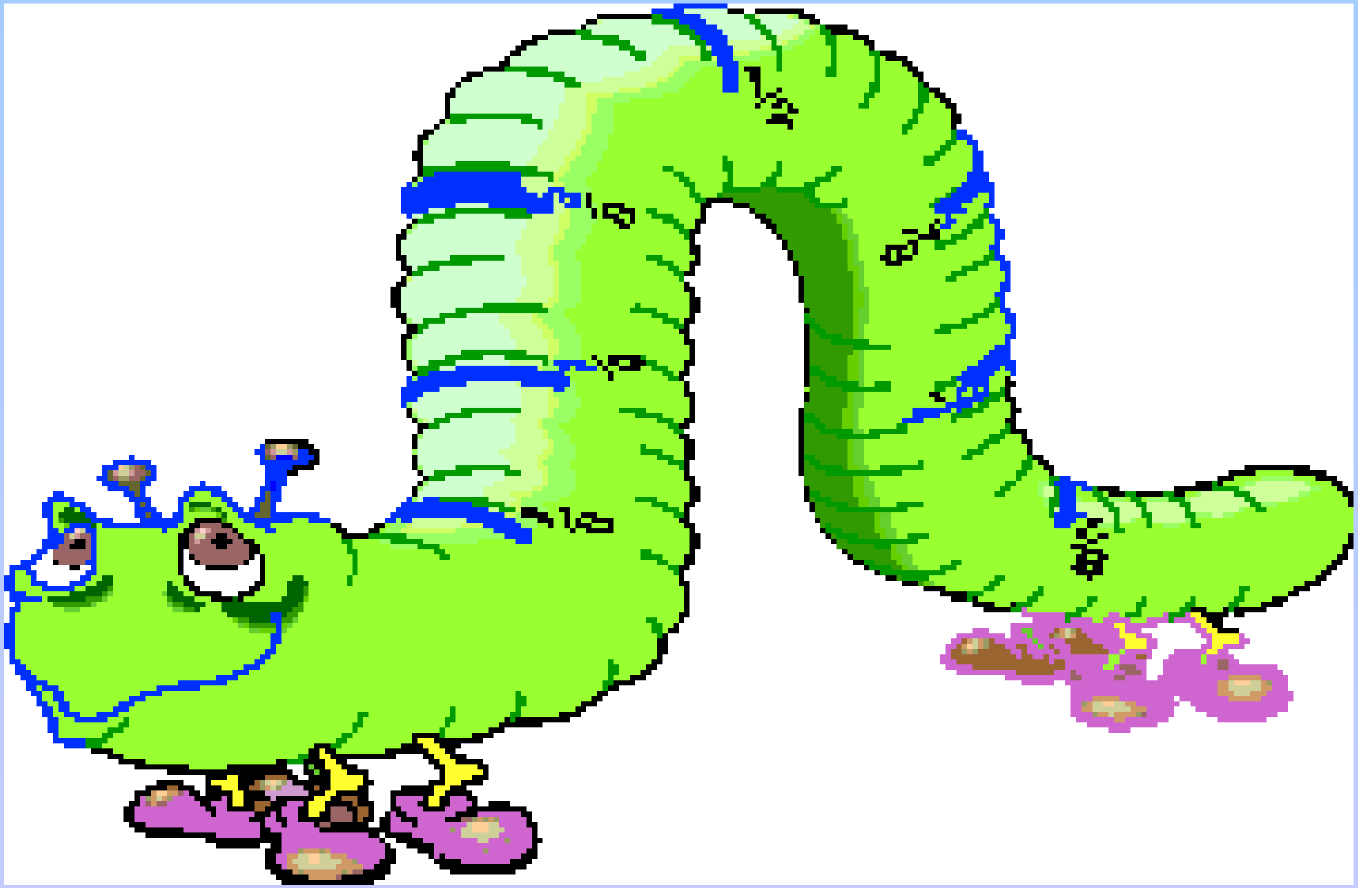
WARNING ** CAUTION ** WARNING ** CAUTION ** WARNING ** CAUTION

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Malicious Code

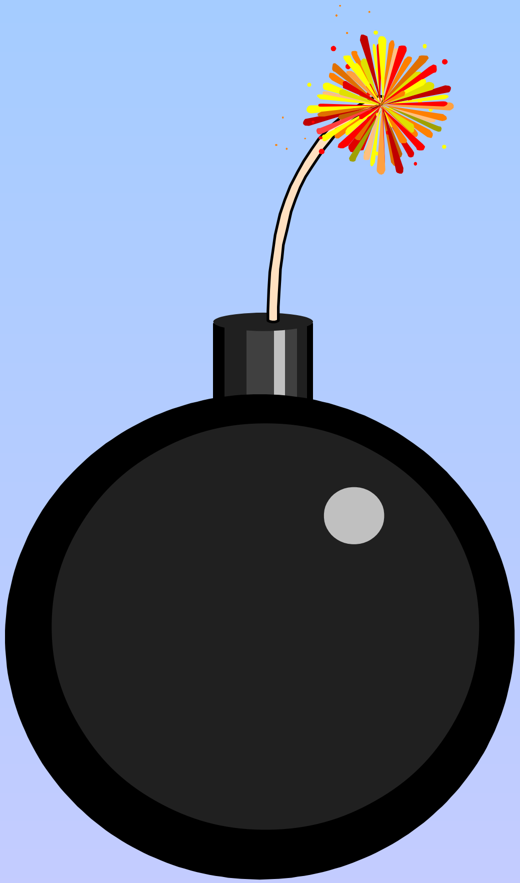
```
NEWLY FORMATTED 3.5 DISKETTE - BOOTABLE
MICHELANGELO INFECTION

Physical Sector: Cyl 0, Side 0, Sector 1

00000000: E6 AA 00 F1 00 70 9A 04  - 03 00 19 9D 00 A0 1C 50   ...............P
00000010: 0A D2 75 1B 33 C0 8E D8  - F6 06 3F 04 01 75 10 58   ..u.3.....?..u.X
00000020: 1F 7C 2D FF 1E 0A 00 9A  - E8 0C 00 9A BA 02 00 58   ..............X
00000030: 1F 2E FF 2E 0A 00 50 53  - 51 52 1E 06 56 57 0E 1F   .....PSQR..VW.
00000040: 0E 07 BE 04 00 B8 01 02  - BB 00 02 B9 01 00 33 D2   ..............3.
00000050: 9C FF 1E 0A 00 73 0C 33  - C0 9C FF 1E 0A 00 4E 75   .....s.3......Nu
00000060: E4 EB 43 33 F6 FC AD 3B  - 07 75 06 AD 3B 47 02 74   ..C3...;.u..;G.t
```

Worm

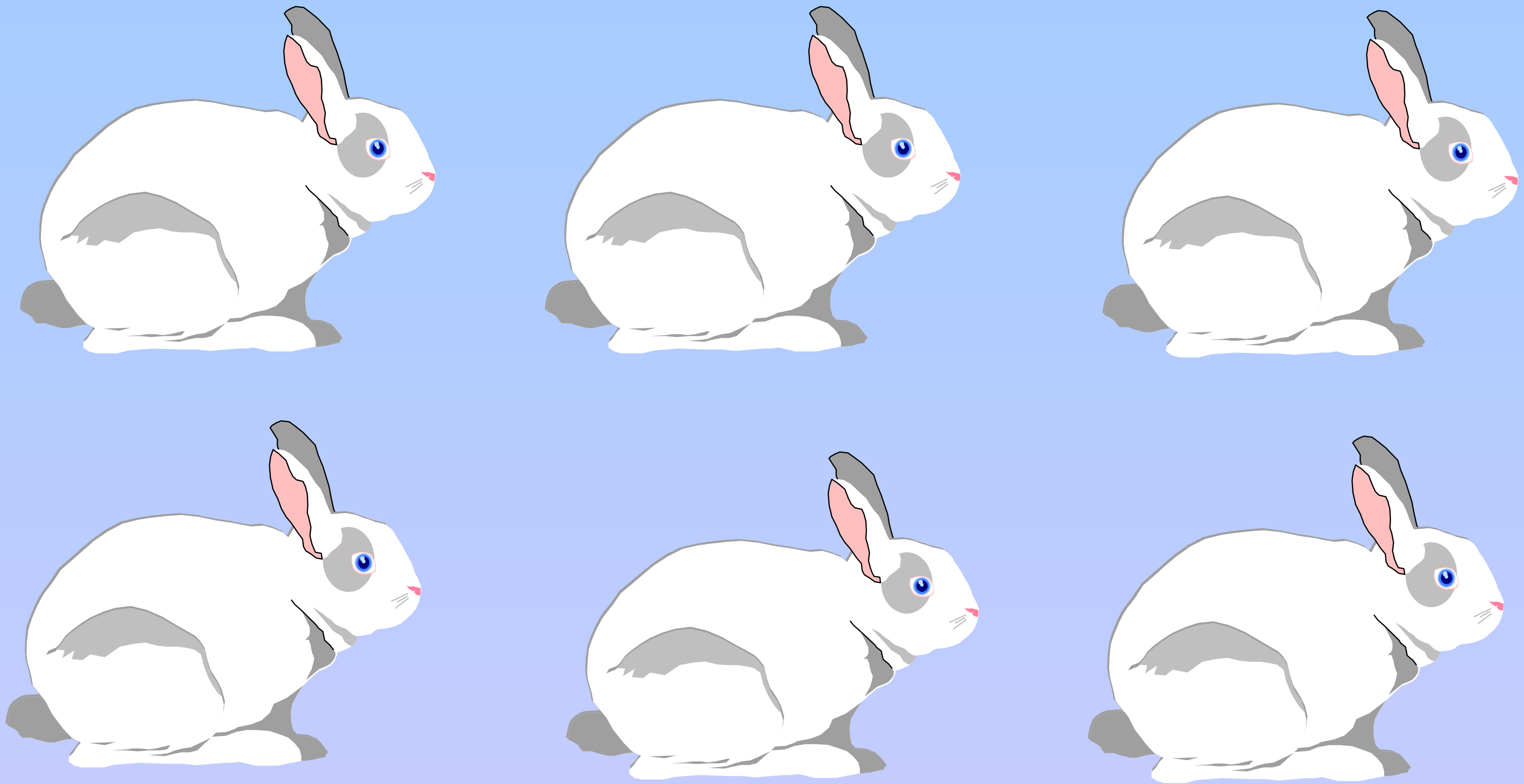


Trojan Horse

Bomb



Virus



Why Viruses Are Successful

- Lack of Awareness
- Absence of Adequate Controls
- Ineffective Use of Existing Controls
- Bugs/Loopholes in System Software
- Unauthorized System Use
- Network Misuse

What is the Cost?

- Labor
- Hardware
- Information Assets
  - Confidentiality
  - Integrity
  - Availability
- Public Relations/Customer Confidence

What Do You Look For?

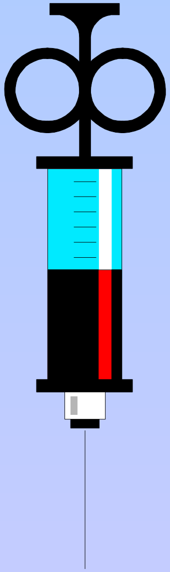
- Note Abnormal or Unexpected Activity
  - Displays, Music or Other Sounds
  - Slowdown in Processing Speed
  - Unusual Disk Activity
  - Error Messages
  - Changes in File Sizes
  - Loss of Programs or Data

If You Suspect an Infection

- STOP Processing
- Take Notes
- Call the ISSO/ISSM

Preventing Infection

- Configure System to Boot From C
- Use Latest Version of Anti-Viral Software
- Scan All Media Before Use
- Scan “New” Computer Systems
- Do Not Use Unapproved Software



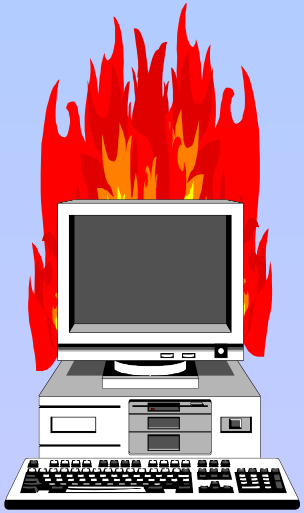
Virus Scanners

- ScanProt
- F-Prot
- IBM Anti-Virus
- McAfee
- Norton Anti-Virus
- Microsoft Anti-Virus

Contingency Plan

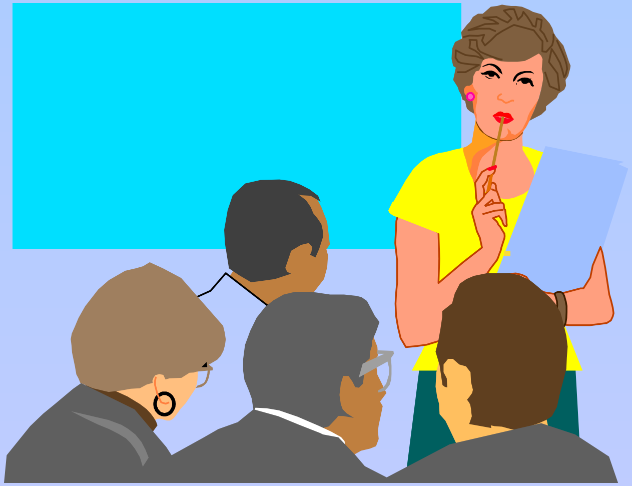
Purpose of Contingency Planning

- Natural Disasters
- Viruses
- Cable Trouble
- Disk Crashes
- Loss of Power
- Hardware Failure
- Security Incidents



Contingency Plan Responsibilities

ISSM



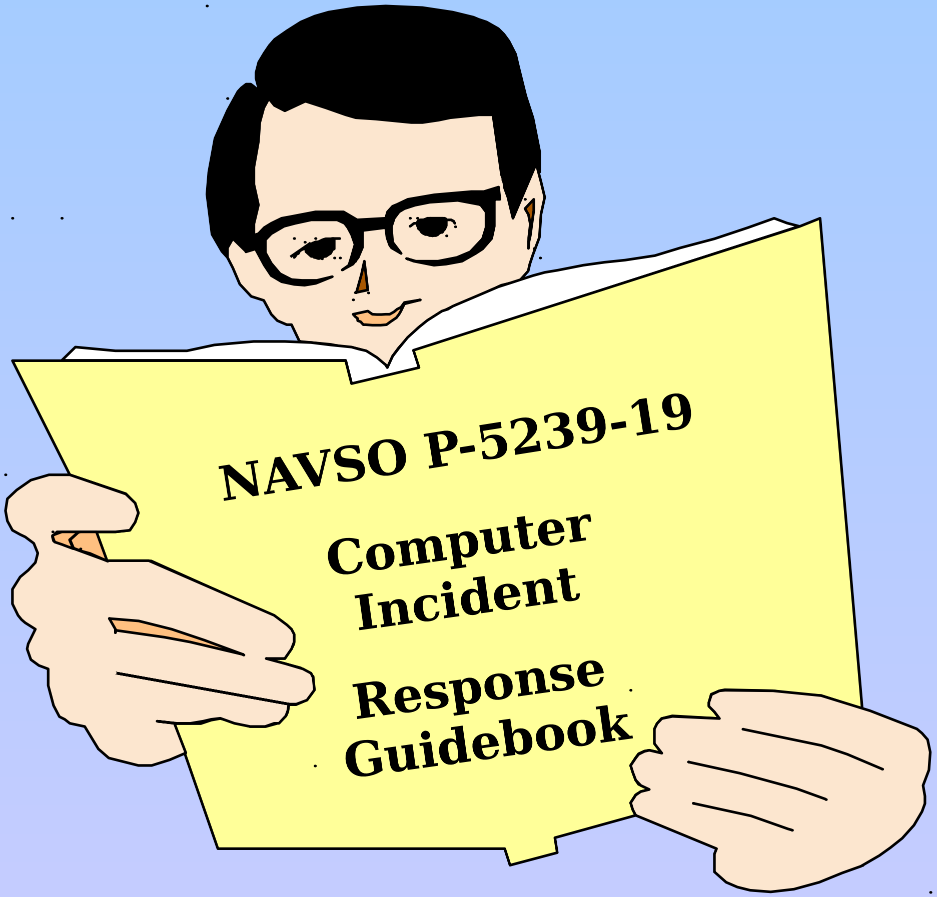
We, The Users

ISSO

Testing Contingency Plans

- Conduct Periodic Testing As Directed
- Perform Evaluation and Update
  - Annually
  - Completion of Risk Assessment
  - Addition of New Application

Computer Incidents



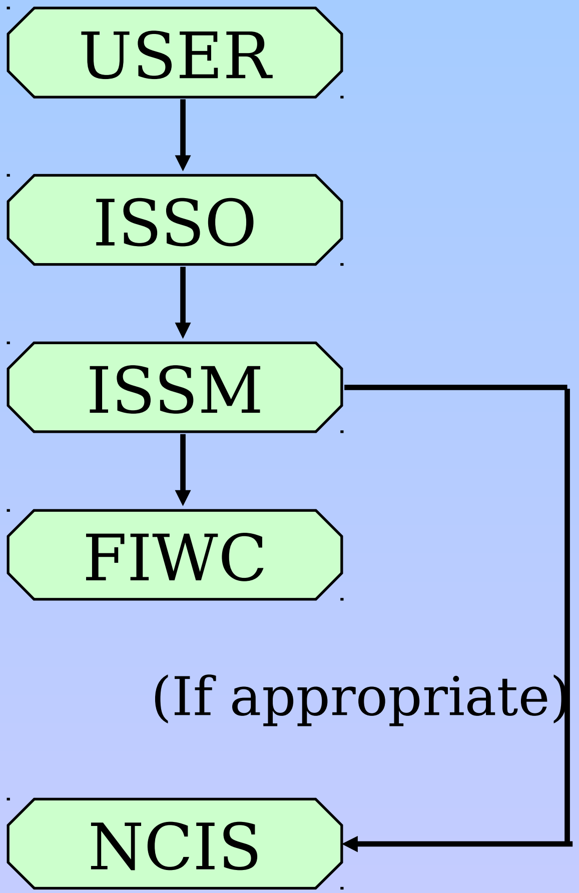
Incident Categories

- Malicious Code Attacks
- Unauthorized Access
- Disruption of Service
- Unauthorized Utilization of Services
- Espionage
- Hoaxes

Responsibilities

- Users
- ISSO/ISSM
- FIWC
  - NAVCIRT
- NCIS
- PAO

Reporting An Incident



Legal Considerations

- Display Warning Banner
- Monitor Systems and Networks
- Do Not Handle Evidence

SUMMARY

In This Lesson We:

- Identified Navy INFOSEC Policies
- Risk Management Procedures
- Discussed Virus Prevention
- Explained Application of Core Valu in INFOSEC